REMARKS

Please reconsider the application in view of the following remarks. Applicants thank the Examiner for carefully considering this application.

Disposition of Claims

Claims 37-49 are pending in this application. Claims 37, 41, and 45 are independent. The remaining claims depend, directly or indirectly, from the independent claims.

Rejections under 35 U.S.C. § 102

"A claim is anticipated only if *each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987) (emphasis added). Further, "[t]he identical invention must be shown in as complete detail as is contained in the claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989).

Claims 37-49 stand rejected under 35 U.S.C. § 102 as being anticipated by U.S. Patent Publication No. 2004/0128392 ("Blakley"). To the extent that this rejection applies to the amended claims, the rejection is respectfully traversed.

Independent claim 37 requires, in part: (i) sending a first authentication request to a first server; (ii) receiving, in response to the first authentication request, an authentication assertion reference from the first server; (iii) sending, to a second server, a request to access the resource operatively connected to the second server, wherein the request comprises the authentication assertion reference; (iv) sending by the second server to the first server, in response to the request, a second authentication request comprising a certificate associated with the second server; (v) determining by the first server, in response to the second authentication request,

whether the certificate is present in a trusted partner list maintained by the first server; (vi) sending by the first server, in response to determining whether the certificate is present in the trusted partner list, an authentication assertion to the second server; and (vii) receiving a grant of access to the resource from the second server, wherein the second server grants access to the resource based on the authentication assertion.

Annotated Figure 7 is included to aid in the understanding at claim 37. It should not be construed as limiting claim 37. Turning to annotated Figure 7, claim 37 discloses a client (710), a first server (715, *i.e.* issuing party), and a second server (740, *i.e.* relying party). Further, the second server (740) is operatively connected to a resource (760). With regards to limitation (i), the client (710) sends a first authentication request to the first server (715). With regards to limitation (ii), the first server (715) sends an authentication assertion reference to the client (710) in response to the first authentication request. With regards to limitation (iii), the client (710) sends to the second server (740) a request to access the resource (760). Limitation (iii) further requires that the request to access the resource (760) includes the authentication assertion reference (provided to the client (710) by the first server (715) in limitation (ii)). With regards to limitation (iv), the second server (740) sends the first server (715) a second authentication request. Limitation (iv) further requires that the second authentication request includes a certificate that is associated with the second server (740). With regards to limitation (v), the first server (715) determines whether the certificate (provided by the second server (740) to the first server (715) in limitation (iv)) is present in a trusted partner list (730) maintained by the first server (715). With regards to limitation (vi), the first server (715) sends an authentication assertion to the second server (740) in response to whether the certificate was present in its trusted partner list (730). With regards to limitation (vii), the second server (740) grants the

client (710) access to the resource (760) based on the authentication assertion (provided by the first server (715) to the second server (740) in limitation (vi)).

For purposes of further clarification, Applicants provide that independent claim 37 is written from the perspective of the client-authenticating first server that, through the issuance of the authentication assertion reference to the client, provides the client with credentials useful in accessing the resources of other servers common to a circle of trust network system. Additionally, independent claims 41 and 45 have similar limitations and are written from the perspectives of the resource-granting second server and the system as a whole, respectively.

Turning to the rejection, Applicants assert that Blakley does not disclose all of the limitations recited in pending independent claim 37 for at least the following reasons.

A Request for a Resource is not a Request for Authentication

Specifically, the Examiner contends that Blakley discloses (i) sending a first authentication request to a first server. *See* Page 3 of the Office Action (citing Figure 3C and paragraph [0138] of Blakley). In doing so, the Examiner has mischaracterized the Blakley reference. The client, as disclosed by Blakley, initiates the process of creating an authentication assertion "when [the] user accesses a link to the relying domain from a Web page or similar resource within the issuing domain." *See* Blakley paragraph [0138]: step 342. Applicants assert that a request made by a client to a first server to access a resource belonging to a second server *is not equivalent to* a request made by a client to a first server for purposes of being authenticated. Accordingly, Blakley cannot be characterized as disclosing limitation (i).

The Authentication Assertion Reference – Who Receives It For Providing to the Relying Server

Further, Blakley does not disclose limitation (ii) which requires receiving, in response to the first authentication request, an authentication assertion reference from the first server. Instead, Blakley discloses "back-end processing at the issuing domain … to build the required assertion" subsequently followed by "the issuing domain [transferring] the assertion along with the user's request to the relying domain." *See* Blakley paragraph [0139]: steps 344-348. Because the authentication assertion is transferred to a relying domain by the issuing domain, and therefore *not* provided to the client in response of the first authentication request, Applicants assert that Blakley also fails to disclose limitation (ii).

A Requesting User's Credentials are not a Relying Server's Certificate

Further, Blakley does not disclose: (iv) sending by the second server to the first server, in response to the request, a second authentication request comprising a certificate associated with the second server; (v) determining by the first server, in response to the second authentication request, whether the certificate is present in a trusted partner list maintained by the first server; and (vi) sending by the first server, in response to determining whether the certificate is present in the trusted partner list, an authentication assertion to the second server. Limitations (iv), (v), and (vi) *all* require the use of a certificate associated with the second server. Applicants assert that Blakley does not disclose the use of a certificate associated with the second server. Rather, the relying server disclosed by Blakley sends client credentials (i.e. username and password) from a relying domain to an issuing domain. *See* Blakley [0157]-[0159]. At best, the user credentials under Blakley identify the user requesting the resource. In contrast, the certificate associated with the second server, as recited in the pending claims, identifies the server

operatively connected to the resource requested by the client. Because the client credentials disclosed by Blakley are not equivalent to the certificate associated with the second server, Blakley does not disclose limitations (iv), (v), and (vi).

A User Registry is not a Trusted Partner List

Further, limitations (v) and (vi) require the use of a trusted partner list. Specifically, limitation (v) discloses a determination as to whether the certificate associated with the second server is present in the trusted partner list. Applicants assert that Blakley does not disclose a trusted partner list. Rather, Blakley uses a registry to verify client credentials. *See* Blakley [0157]-[0159]. Conceptually, a client is distinct from a server that is a trusted partner in a circle of trust network because the client at best is the entity requesting a resource while a trusted partner is the server entity associated with the resource. *See* paragraph [0045] and Figure 7 of the published application. Accordingly, the user registry disclosed by Blakley for verification of a resource-requesting user's credentials cannot be equated to a trusted partner list used for verification of a resource-granting server's certificate. For at least that reason, Blakley does not disclose limitations (v) and (vi).

In view of the above, Blakley fails to disclose all the limitations of claim 37. Further, independent claims 41 and 45 have similar limitations and are therefore patentable for at least the same reasons. Dependent claims are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicants believe this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 03226 / 503001).

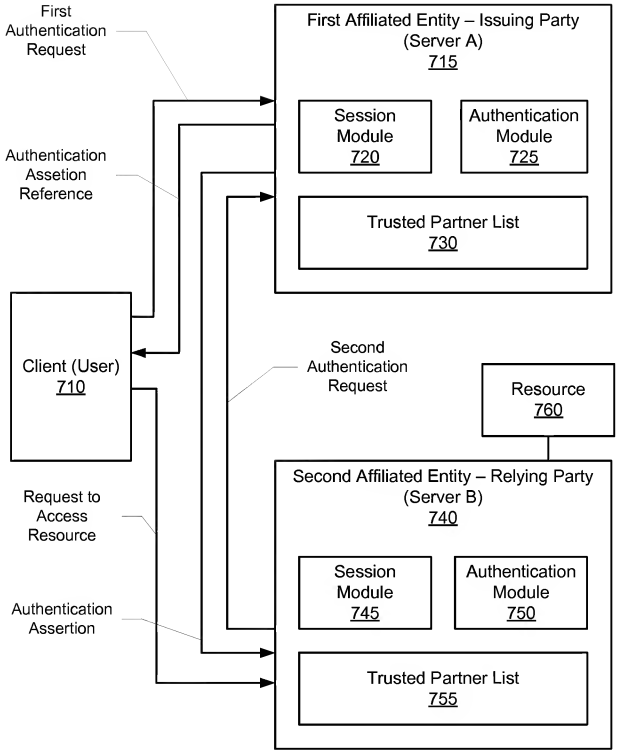
Dated: February 18, 2009

Respectfully submitted,

By /Robert P. Lord/

Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
909 Fannin Street, Suite 3500
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicants

Attachment: Annotated Figure 7



ANNOTATED FIGURE 7